DOD VULNERABILITY DISCLOSURE PROGRAM
BUG BYTES JUNE 2022
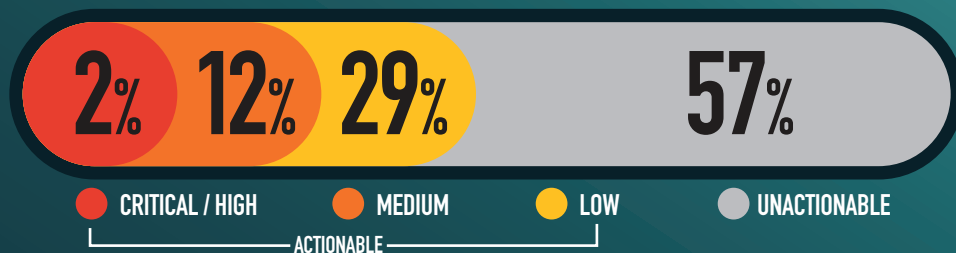
41,012
VULNERABILITIES SINCE LAUNCH

3,421
RESEARCHERS SINCE LAUNCH

23,671
ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH

| 2% | 12% | 29% | 57% |

- CRITICAL / HIGH
- MEDIUM
- LOW
- UNACTIONABLE

ACTIONABLE

SUBMITTED VULNERABILITIES

	DEC 2021	JAN 2022	FEB 2022	MAR 2022	APR 2022	MAY 2022	JUN 2022
Value	443	708	981	859	446	359	252

LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-200 INFORMATION DISCLOSURE — 104

CWE-284 IMPROPER ACCESS CONTROL - GENERIC — 36

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES — 32

CWE-79 CROSS-SITE SCRIPTING (XSS) — 18

KNOWLEDGE BYTE

In June 2022, the DoD VDP received a critical finding regarding CVE-2021-34473, a Server-Side Request Forgery (SSRF) leading to Remote Code Execution (RCE). This vulnerability exists in Microsoft Exchange due to improper input validation, allowing an attacker to execute arbitrary code on the system. JFHQ-DODIN is not aware of any DoD-related incidents; however, system administrators should refer to the Microsoft Security Update Guide (July 2021) for affected applications and appropriate patches.

More information can be found at the following:
https://msrc.microsoft.com/update-guide/en-us
https://iavm.csd.disa.mil/iavm-notice-html/143647
https://peterjson.medium.com/reproducing-the-proxyshell-pwn2own-exploit-49743a4ea9a1

RESEARCHER OF THE MONTH

The DoD VDP Researcher of the Month for June 2022 is **@0xhunster**. They submitted a critical report on pre-auth SSRF of a DoD exchange server that could lead to RCE with CVE-2021-34473. Thank you very much! VDP Hackers for the win!

DC3
DOD CYBER CRIME CENTER